UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/917,368	07/27/2001	Jeffrey Scott Bardsley	RSW920010137US1	1486

7590 07/14/2005

Duke Yee
Yee & Asscoiates P C
4100 Aipha Road
Suite 1100
Dallas, TX 75244

EXAMINER	
POPHAM, JEFFREY D	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 07/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/917,368	BARDSLEY ET AL.	
	Examiner	Art Unit	
	Jeffrey D. Popham	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 April 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *5-11 and 15-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *5-11 and 15-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 July 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Remarks

Claims 5-11 and 15-27 are pending.

Response to Arguments

1. Applicant's arguments, see pages 8-9, section 3 of the remarks, filed 4/26/2005, with respect to the rejection of claims 5-11 and 15-20 under 35 U.S.C. 103(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection with Yavatkar is made in view of Skirmont et al. (U.S. Patent 6,553,005).

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. Claims 5-11 and 15-20 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. For purposes of prior art rejection, the preamble of claim 5 has been construed as "A computer-implemented method of identifying the entry point...".

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 5-11, 15, 18, and 20-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yavatkar et al. (U.S. Patent 6,735,702) in view of Skirmont et al. (U.S. Patent 6,553,005).

Regarding Claim 5,

Yavatkar discloses a computer-implemented method of identifying the entry point of an attack upon a device protected by an intrusion detection system, the method comprising the steps of:

Obtaining intrusion information, from an intrusion detection system, regarding an attack upon a device protected by the intrusion detection system (watchdog agent) (Column 15, lines 4-17);

Obtaining network information, from network equipment connected to the device, regarding the attack (Column 17, lines 32-51);

Determining a logical entry point of the attack using a correlation engine to correlate the intrusion information and the network information (Column 18, lines 32-53);

And that the entry point is associated with a port (Column 18, lines 19-31);

But do not disclose identifying a physical port associated with the logical port.

Skirmont, however, discloses identifying a physical port associated with the logical port (Column 2, lines 6-19). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the logical to physical port mapping of Skirmont into the intrusion detection system of Yavatkar because it is well known in the art or in order to allow for proper routing table modifications that will prevent attack traffic from entering the network (Yavatkar: Column 21, lines 28-35).

Regarding Claim 6,

Yavatkar discloses that the intrusion information includes an address (Column 15, lines 18-21).

Regarding Claim 7,

Yavatkar discloses that the address is a source address (Column 15, lines 18-21).

Regarding Claim 8,

Yavatkar discloses that the address is a destination address (Column 15, lines 50-65).

Regarding Claim 9,

Yavatkar discloses that the network information includes a logical port identifier of a logical port associated with the address (Column 17, lines 38-39).

Regarding Claim 10,

Yavatkar discloses that the step of determining a logical entry point includes the step of finding, in the network information, the logical port identifier of the logical port associated with the address (Column 17, lines 32-51).

Regarding Claim 11,

Skirmont discloses identifying a physical port associated with the logical port (Column 2, lines 6-19).

Regarding Claim 15,

Yavatkar discloses that the network equipment includes a firewall with routing function (Column 18, lines 54-62).

Regarding Claim 18,

Yavatkar discloses that the intrusion detection system includes network based intrusion detection equipment (Column 15, lines 4-17).

Regarding Claim 20,

Yavatkar discloses that the intrusion detection system includes application based intrusion detection equipment (Column 3, lines 38-45).

Regarding Claim 25,

Yavatkar discloses an apparatus for detecting a point of an attack on a network, the apparatus comprising:

Network equipment for connecting a protected device to a network (Column 15, lines 4-17);

An intrusion detection system comprising intrusion detection equipment (Column 15, lines 4-17);

A correlation engine adapted to:

Receive a notification of an attack on the protected device (Column 15, lines 4-17);

Receive intrusion information regarding the attack (Column 15, lines 4-17; and Column 18, lines 32-53);

Receive network information regarding the attack, wherein the network information pertains to the network (Column 17, lines 32-51; and Column 18, lines 32-53);

Correlate the intrusion information and the network information to produce correlation information (Column 18, lines 32-53);

Find on the network a logical port of connection used by the attack (Column 18, lines 32-53);

But does not disclose mapping the logical port on the network to a physical port on the network.

Skirmont, however, discloses mapping the logical port on the network to a physical port on the network (Column 2, lines 6-19). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the logical to physical port mapping of Skirmont into the intrusion detection system of Yavatkar because it is well

known in the art or in order to allow for proper routing table modifications that will prevent attack traffic from entering the network (Yavatkar: Column 21, lines 28-35).

Regarding Claim 21,

Claim 21 is a method claim that corresponds to system claim 25 and is rejected for the same reasons.

Regarding Claim 23,

Claim 23 is a method claim that corresponds to system claim 25 and is rejected for the same reasons.

Regarding Claim 26,

Yavatkar discloses means for alerting a network manager to the location of the logical port (Column 18, line 54 to Column 19, line 6) and Skirmont discloses mapping the logical port to a physical port (Column 2, lines 6-19).

Regarding Claim 22,

Claim 22 is a method claim that corresponds to system claim 26 and is rejected for the same reasons.

Regarding Claim 27,

Yavatkar discloses that the intrusion information includes an address (Column 15, lines 18-21) and the network information includes a logical port identifier of a logical port associated with the address (Column 17, lines 38-39).

Regarding Claim 24,

Claim 24 is a method claim that corresponds to system claim 27 and is rejected for the same reasons.

4. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Yavatkar in view of Skirmont, further in view of ND ("Network Dispatcher: a connection router for scalable Internet services", 10/2/1998, Internet Security Systems, obtained from http://www.unizh.ch/home/mazzo/reports/www7conf/fullpapers/1899/com1899.htm).

Yavatkar as modified by Skirmont does not disclose that the network equipment includes a network dispatcher.

ND, however, discloses that the network equipment includes a network dispatcher (Pages 1-2, Introduction, Paragraphs 1-4). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the network dispatcher of ND into the intrusion detection system of Yavatkar as modified by Skirmont in order to spread the load of the network evenly upon multiple servers or nodes of the network.

5. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Yavatkar in view of Skirmont, further in view of Shanklin et al. (U.S. Patent 6,578,147).

Yavatkar as modified by Skirmont does not disclose that the network equipment includes a load balancer.

Shanklin, however, discloses that the network equipment includes a load balancer (Column 7, lines 39-47). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the load balancer of Shanklin into the intrusion detection system of Yavatkar as modified by Skirmont in order to distribute traffic so that each intrusion detection agent processes only a portion of the traffic.

6. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Yavatkar in view of Skirmont, further in view of NVHIDS ("Network- vs. Host-based Intrusion Detection", April 1998, Proceedings of the 7th International World Wide Web Conference (WWW7), obtained from http://documents.iss.net/whitepapers/nvh_ids.pdf).

Yavatkar as modified by Skirmont does not disclose that the intrusion detection system includes host based intrusion detection equipment.

NVHIDS, however, discloses that the intrusion detection system includes host based intrusion detection equipment (Page 9, Paragraph 1). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the host based intrusion detection of NVHIDS into the intrusion detection system of Yavatkar as modified by Skirmont in order to improve network resistance to attacks and misuse, enhance enforcement of security policy, and introduce greater flexibility in deployment options.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey D. Popham whose telephone number is (571)-272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137